Recipe 20 - Configuration Guide for Setting up Netegrity eTRust SiteMinder 6.0.1.04 as an AA and CS

Table of Contents:

Version 2.0.0

1 Setup

1.1 Terms and Introduction

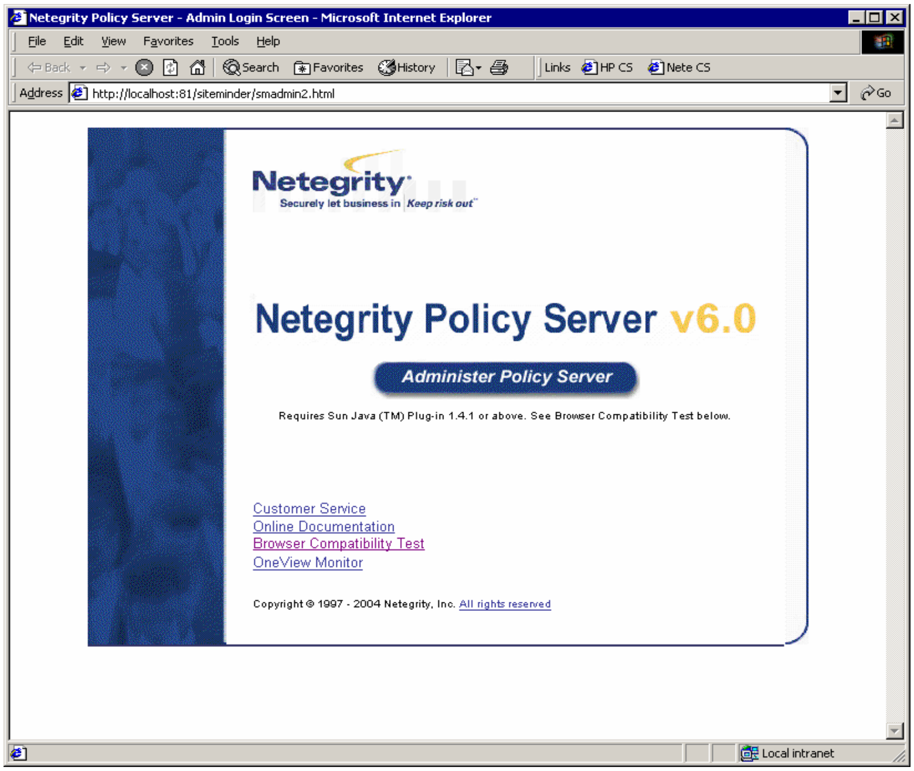
The SAML 1.0 is one of the adopted schemes within the E-Authentication architectural framework. This guide should help you setup SAML 1.0 and Netegrity eTRust SiteMinder 6.0.1.04 as an Agency Application (AA) and Credential Service (CS). Remember that the Netegrity eTRust SiteMinder setup screens are often the same, whether setting up an AA or a CS. After reviewing the terms, configure your scheme to handle SAML 1.0, starting at the login page shown in Figure 20-1.

Term	Definition
Agency Application (AA)	An online service provided by a government agency that requires an end user to be authenticated.
Credential Service (CS)	A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential, then each one is considered a separate CS.
Credential Service Provider (CSP)	An organization that offers one or more CSs. Sometimes known as an Electronic Credential Provider (ECP).
Project Management Office (PMO)	The PMO is the organization that handles E-Authentication program management, administration, and operations.

2 Partner Configuration

2.1 Open Netegrity Policy Server 6.0

Open Netegrity Policy Server 6.0 by clicking on **Start** > **Programs** > **SiteMinder** > **Netegrity Policy Server User Interface**. Netegrity Policy Server 6.0 screen should appear as shown in Figure 20-1. Next, click on the **Administer Policy Server**.

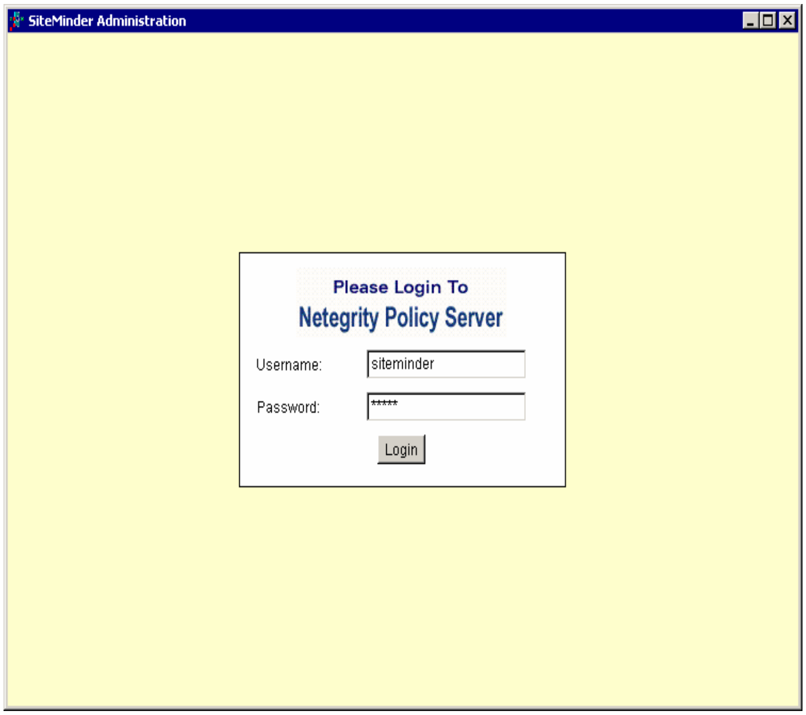

Netegrity Policy Server - Admin Login Screen - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links HP CS Nete CS
Address http://localhost:81/siteminder/smadmin2.html
Go
Netegrity
Securely let business in Keep risk out
Netegrity Policy Server v6.0
Administer Policy Server
Customer Service
Online Documentation
Browser Compatibility Test
OneView Monitor
Local intranet

Requires Sun Java (TM) Plug-in 1.4.1 or above. See Browser Compatibility Test below.

Copyright © 1997 - 2004 Netegrity, Inc. All rights reserved

Figure 20-1: Netegrity Policy Server 6.0

The SiteMinder Administration login screen should appear as shown in Figure 20-2. Enter a valid **Username** and **Password** and click the **Login** button.



Username: siteminder

Password: *****

Figure 20-2: SiteMinder Administration Login Screen

2.2 Configure a Partner AA

Once you have successfully logged into the application, the SiteMinder 6.0 Administration screen will appear as shown in Figure 20-3.

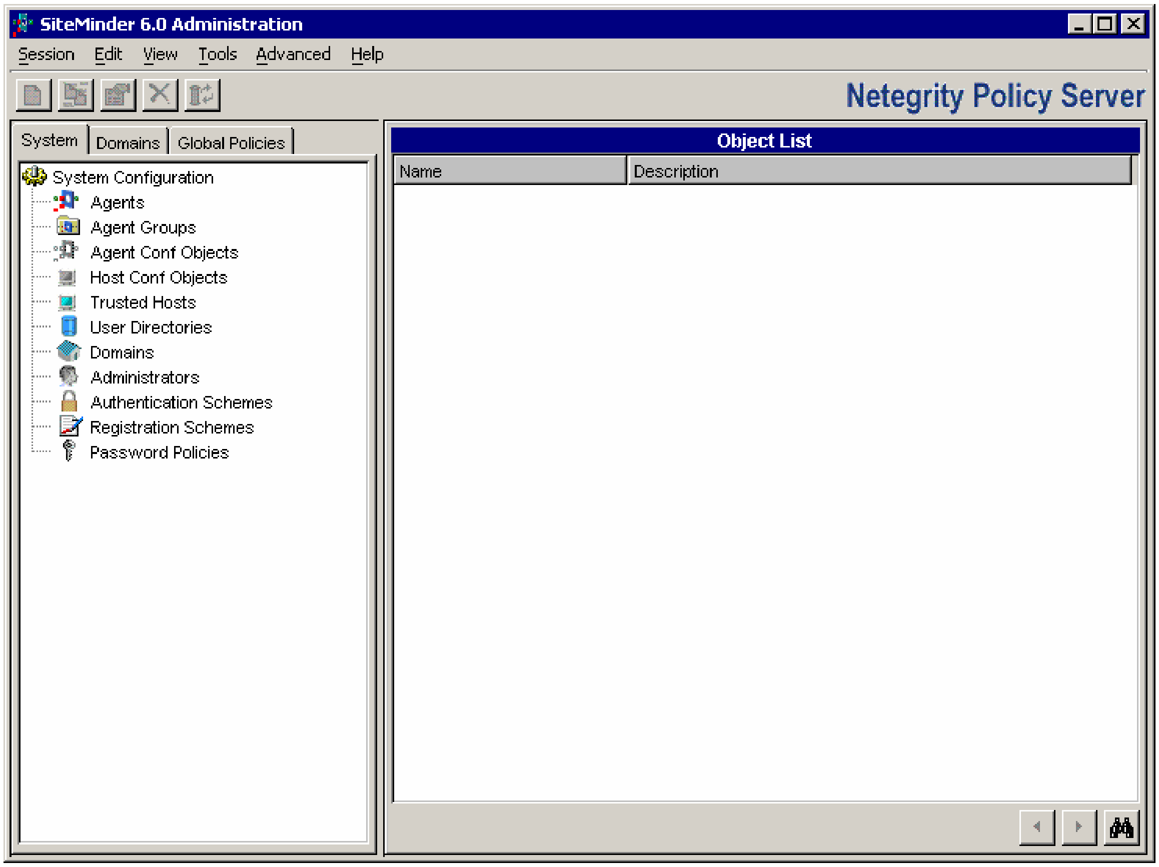
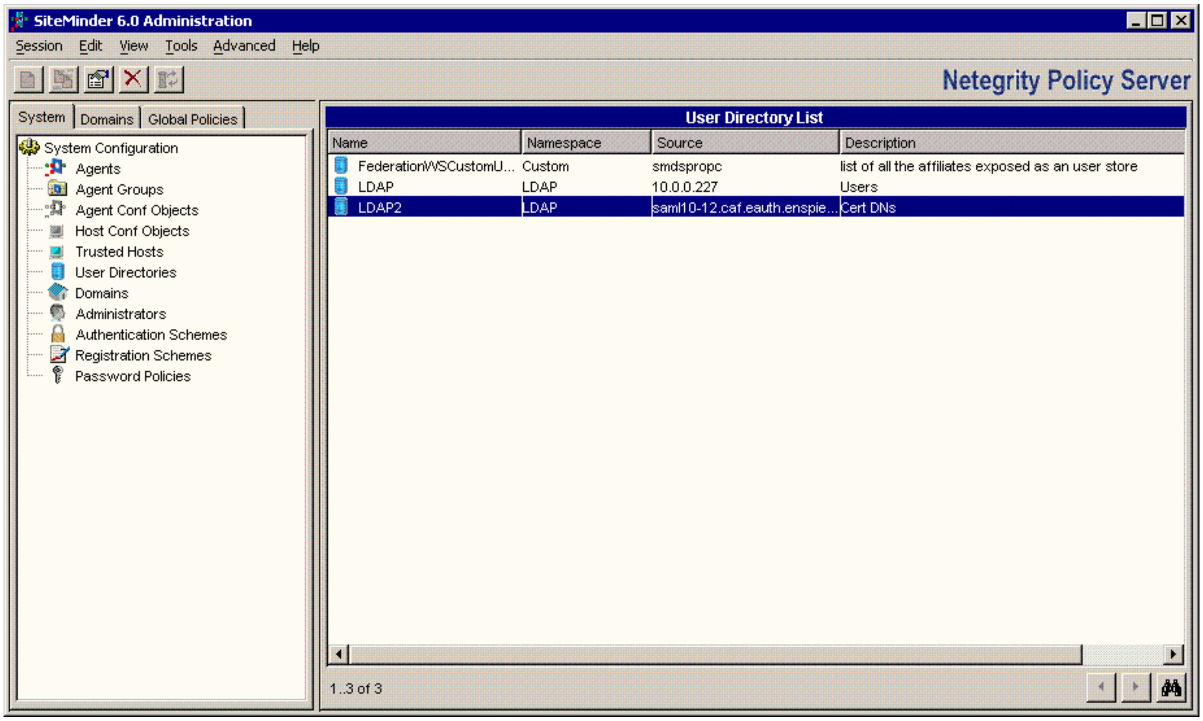


Figure 20-3: SiteMinder 6.0 Administration Screen

The Lab has used LDAP to store information on client certificates, although that is not the only method possible. First, verify that LDAP directory resources have been defined for Certificates. This is accomplished by clicking on the **System** tab (left side of the Administration screen) and then selecting **User Directories**. The User Directory List screen will appear as shown in Figure 20-4. To create a new Directory resource right click on **User Directories** and select **Create Directory**.

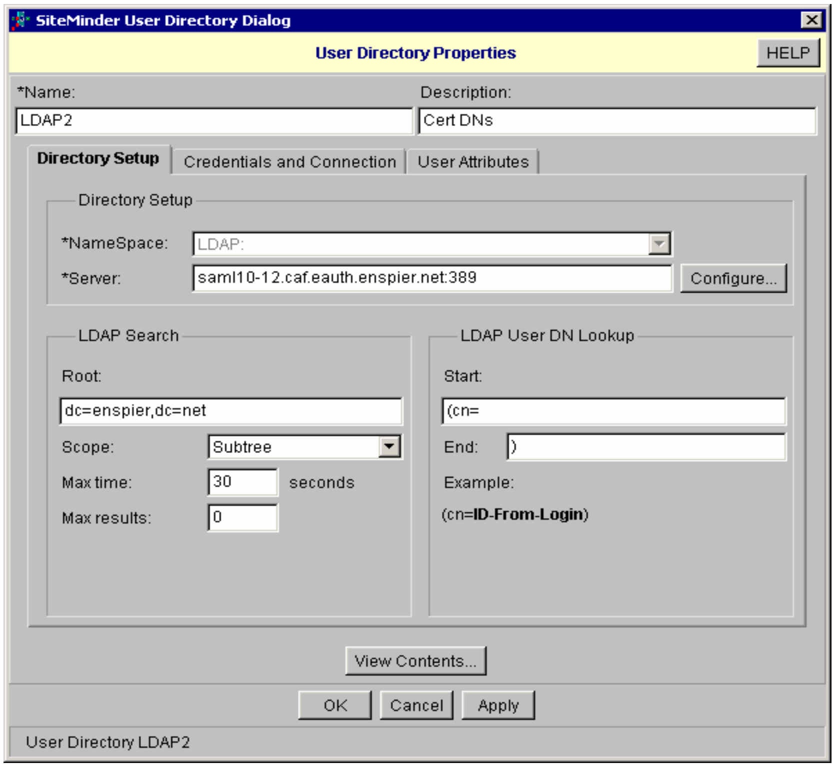


User Directory List

Name	Namespace	Source	Description
FederationWSCustomU...	Custom	smdspropc	list of all the affiliates exposed as an user store
LDAP	LDAP	10.0.0.227	Users
LDAP2	LDAP	saml10-12.caf.eauth.enspie...	Cert DNs

Figure 20-4: User Directory List

If creating a Directory has been chosen, the User Directory Properties screen will appear as shown in Figure 20-5. Provide all necessary configuration information as demonstrated below. The **LDAP User DN Lookup** area is important for configuration. Next, enter the values for **Start** and **End** as shown in Figure 20-5 and then select **Apply**. This is how the Lab maps the subject of the certificate to a "user" in the LDAP store.



*Name: LDAP2

Description: Cert DNs

*NameSpace: LDAP:

*Server: saml10-12.caf.eauth.enspier.net:389

Root: dc=enspier,dc=net

Scope: Subtree

Max time: 30 seconds

Max results: 0

Start: (cn=

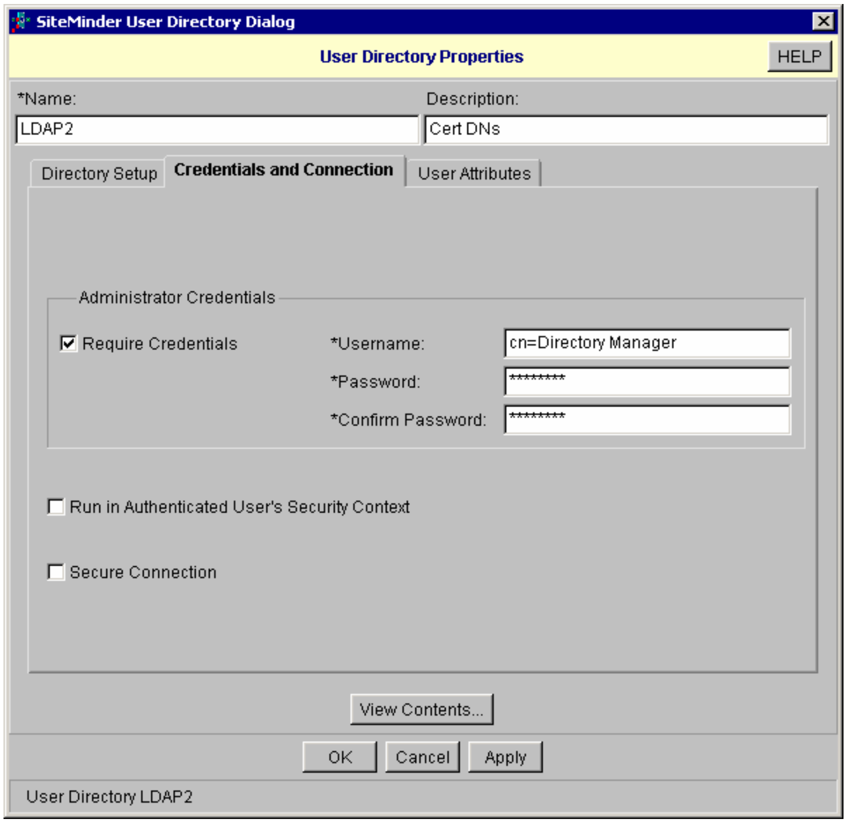
End:)

Example: (cn=**ID-From-Login**)

User Directory LDAP2

Figure 20-5: User Directory Properties – Directory Setup

Next, select **Credentials and Connection** tab from the User Directory Properties screen as shown in Figure 20-6. Provide all necessary configuration information as demonstrated below. Be sure you have entered the correct credentials for the LDAP store.


SiteMinder User Directory Dialog
User Directory Properties
HELP
Directory Setup
Credentials and Connection
User Attributes
Administrator Credentials
View Contents...
OK
Cancel
Apply

*Name: LDAP2

Description: Cert DNs

☑ Require Credentials

*Username: cn=Directory Manager

*Password: ********

*Confirm Password: ********

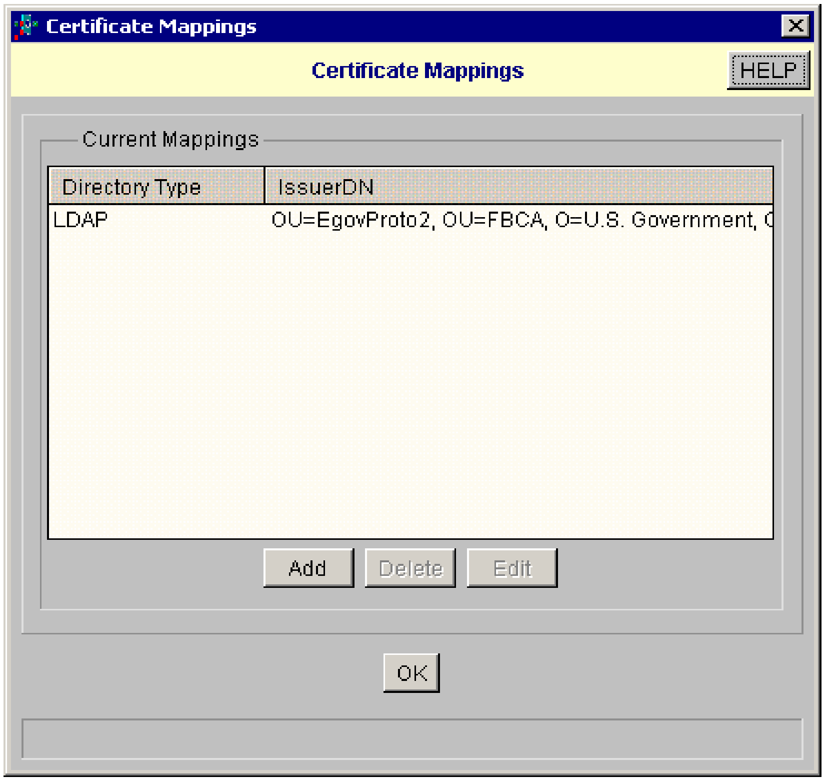
□ Run in Authenticated User's Security Context

□ Secure Connection

User Directory LDAP2

Figure 20-6: Credentials and Connections

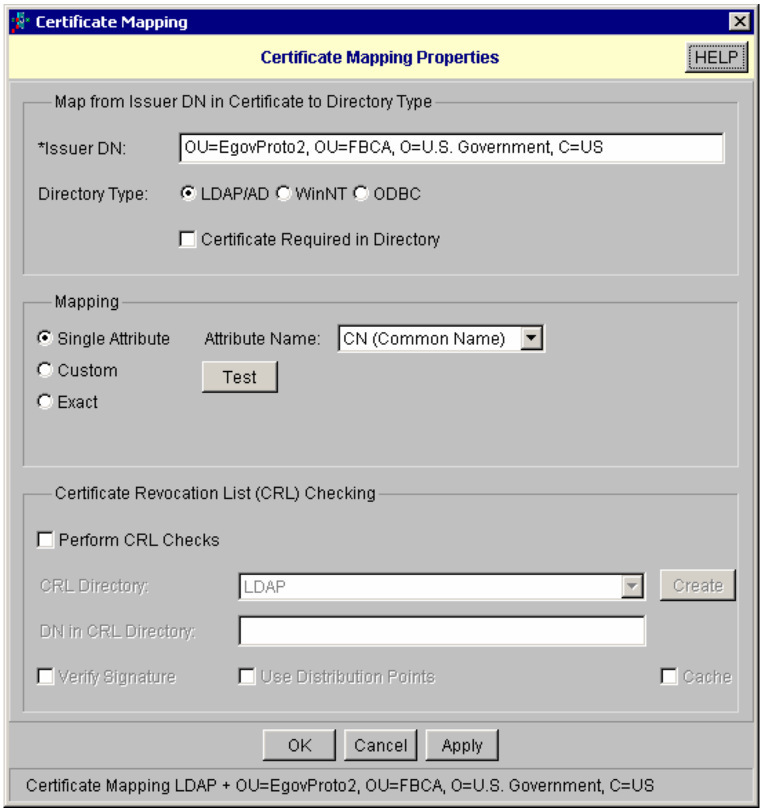
Next, you must verify that the certificate mapping rules are in place. This is completed by going to the SiteMinder 6.0 Administration screen (Figure 20-3) and clicking on **Advanced > Certificate Mapping.** The Certificate Mappings screen will appear as shown in Figure 20-7.   To add a certificate mapping, select the **Add** button.



Directory Type	IssuerDN
LDAP	OU=EgovProto2, OU=FBCA, O=U.S. Government, C

Figure 20-7: Certificate Mappings

The Certificate Mapping Properties screen will appear as shown in Figure 20-8. This screen provides an example of a mapping. Provide all appropriate configuration information as demonstrated below. The **Issuer DN** is taken from your client's (AA) certificate in the issuer field. Be sure to select **LDAP/AD**, **Single Attribute**, and **CN (Common Name)** as shown in Figure 20-8. Select **OK** when these steps have been completed.



Certificate Mapping

Certificate Mapping Properties

Map from Issuer DN in Certificate to Directory Type

*Issuer DN: OU=EgovProto2, OU=FBCA, O=U.S. Government, C=US

Directory Type: ● LDAP/AD ○ WinNT ○ ODBC

□ Certificate Required in Directory

Mapping

● Single Attribute Attribute Name: CN (Common Name)

○ Custom

○ Exact

Certificate Revocation List (CRL) Checking

□ Perform CRL Checks

CRL Directory: LDAP

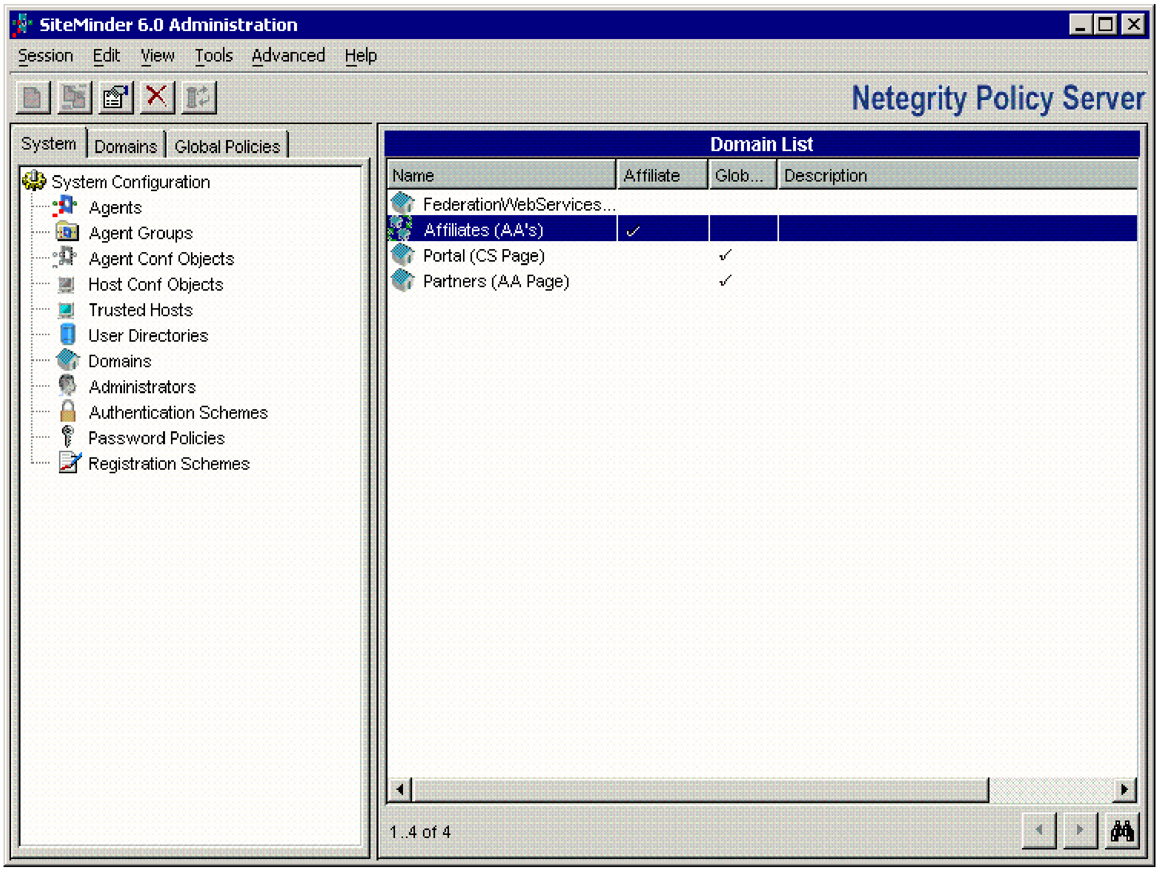
DN in CRL Directory:

□ Verify Signature □ Use Distribution Points □ Cache

Certificate Mapping LDAP + OU=EgovProto2, OU=FBCA, O=U.S. Government, C=US

Figure 20-8: Certificate Mapping Properties

Next, verify that the created LDAP resources have been added to the Affiliates container. This accomplished by clicking on the **System** tab and selecting **Domains**. The Domain List screen will appear as shown in Figure 20-9. To view its properties double clicking on **Affiliates** as demonstrated below.

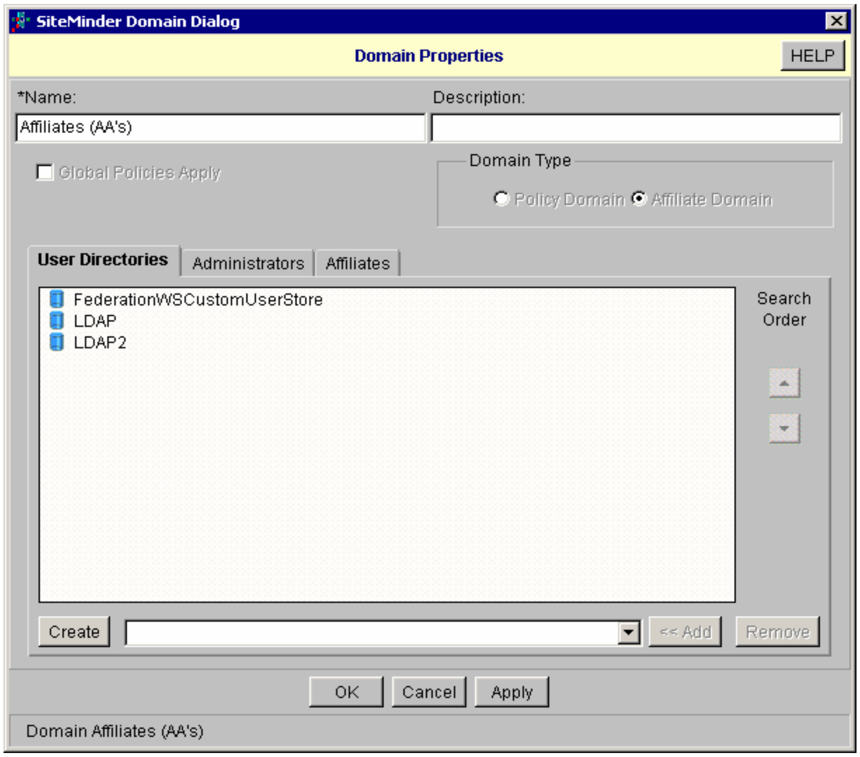


Domain List

Name	Affiliate	Glob...	Description
FederationWebServices...			
Affiliates (AA's)	✓		
Portal (CS Page)		✓	
Partners (AA Page)		✓	

Figure 20-9: Domain List

The Domain Properties screen will appear as shown in Figure 20-10. The created LDAP resource should be listed under the **User Directories** tab.



*Name: Affiliates (AA's)

Description:

□ Global Policies Apply

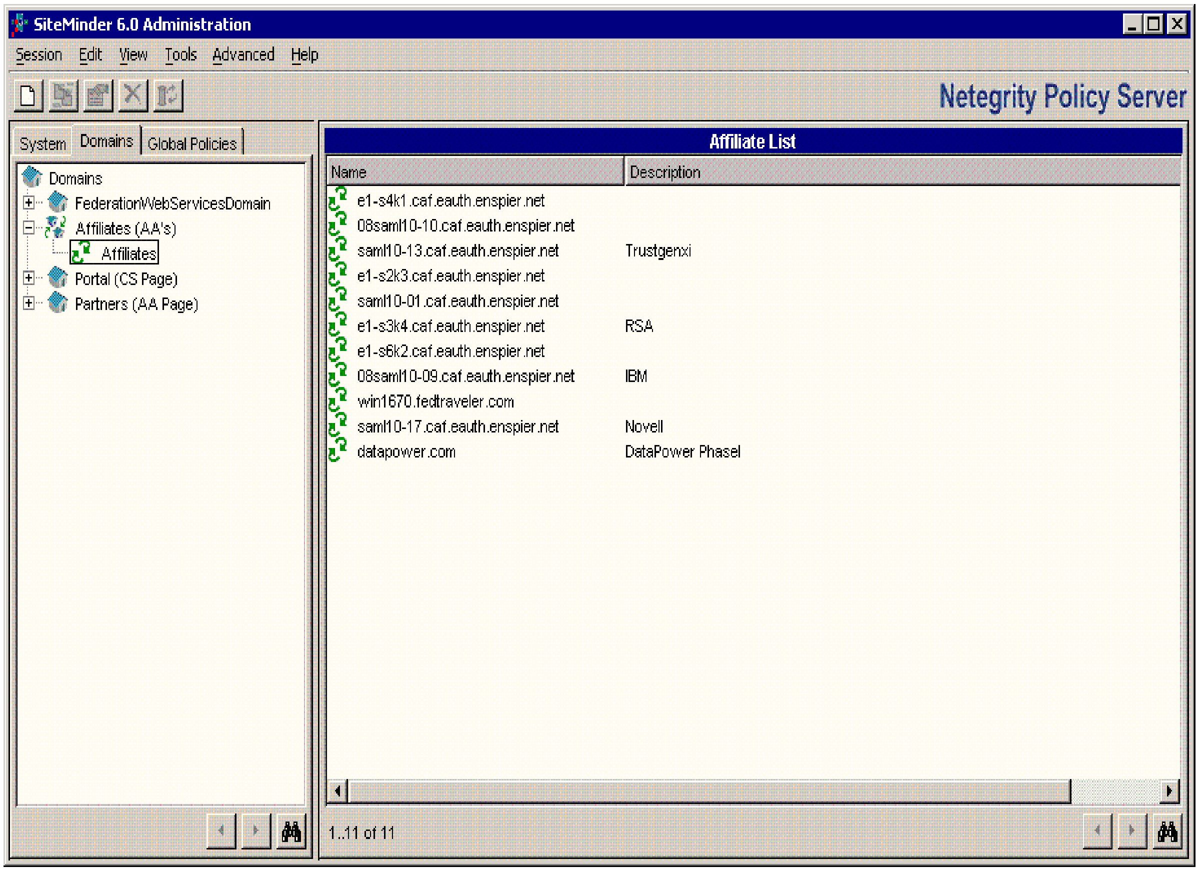
Domain Type: ○ Policy Domain ● Affiliate Domain

FederationWSCustomUserStore
LDAP
LDAP2

Domain Affiliates (AA's)

Figure 20-10: Domain Properties

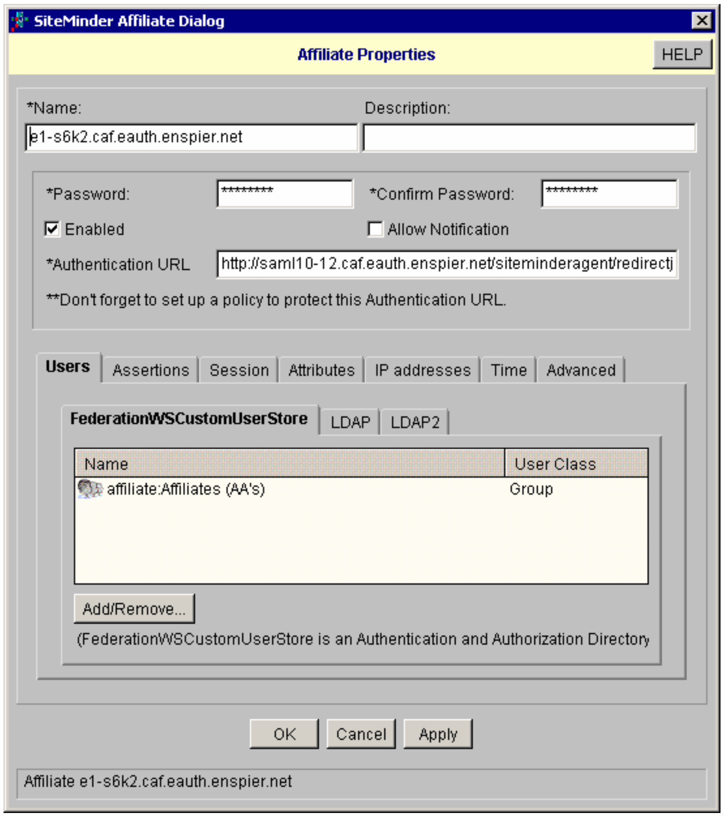
Next, you will need to define the affiliate properties. This is done by clicking on the **Domains** tab (left side of the SiteMinder Administration screen) and then selecting **Attributes > Affiliates** as demonstrated in Figure 20-11. To add an affiliate, right click on **Affiliates** and select **Create Affiliate**. Be sure to make the affiliate name the same as the CN from the subject of their client certificate.


SiteMinder 6.0 Administration
Session Edit View Tools Advanced Help
Netegrity Policy Server
System Domains Global Policies
Domains
FederationWebServicesDomain
Affiliates (AA's)
Affiliates
Portal (CS Page)
Partners (AA Page)
Affiliate List
1..11 of 11

Name	Description
e1-s4k1.caf.eauth.enspier.net	
08saml10-10.caf.eauth.enspier.net	
saml10-13.caf.eauth.enspier.net	Trustgenxi
e1-s2k3.caf.eauth.enspier.net	
saml10-01.caf.eauth.enspier.net	
e1-s3k4.caf.eauth.enspier.net	RSA
e1-s6k2.caf.eauth.enspier.net	
08saml10-09.caf.eauth.enspier.net	IBM
win1670.fedtraveler.com	
saml10-17.caf.eauth.enspier.net	Novell
datapower.com	DataPower Phasel

Figure 20-11: Affiliate List

The Affiliate Properties screen will appear as shown in Figure 20-12. There are three (3) User sub tabs that need to be set. As demonstrated below, click on the **Federation/WSCustomUserStore** tab and provide the appropriate configuration information.



*Name: e1-s6k2.caf.eauth.enspier.net

Description:

*Password: ********

*Confirm Password: ********

☑ Enabled

□ Allow Notification

*Authentication URL: http://saml10-12.caf.eauth.enspier.net/siteminderagent/redirectj

**Don't forget to set up a policy to protect this Authentication URL.

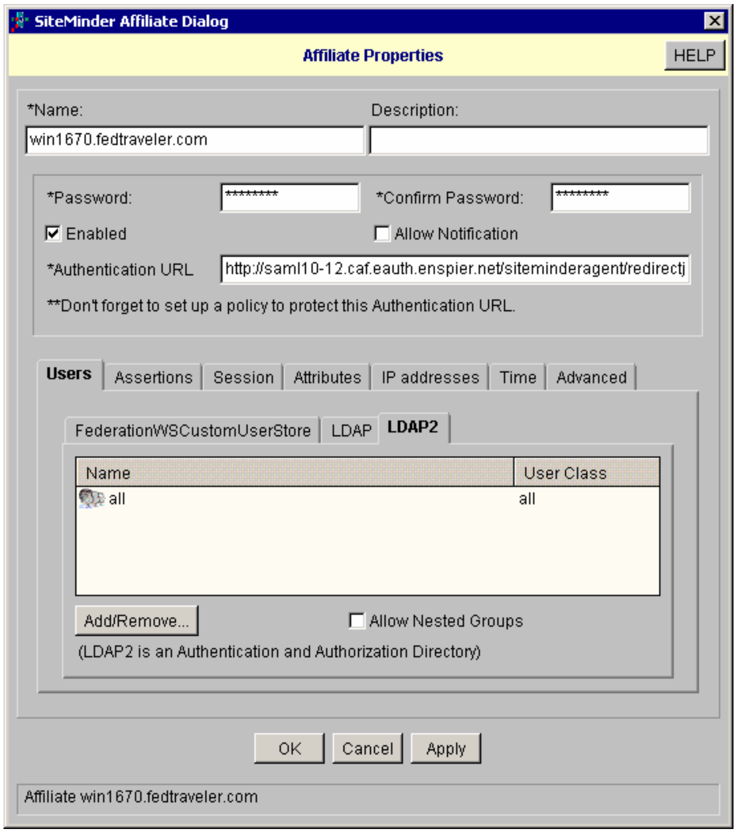
Name	User Class
affiliate:Affiliates (AA's)	Group

(FederationWSCustomUserStore is an Authentication and Authorization Directory

Affiliate e1-s6k2.caf.eauth.enspier.net

Figure 20-12: Affiliate Properties - FederationWSCustomUserStore

Next, set the value for LDAP2 by clicking on the **LDAP2** tab. As shown in Figure 20-13, the Lab sets LDAP2 to **all**. You will probably want to be more specific. The LDAP2 tab was defined in the “User Directory” step above. To add a user or group of users, select the **Add/Remove** button.



*Name: win1670.fedtraveler.com

Description:

*Password: ********

*Confirm Password: ********

☑ Enabled

□ Allow Notification

*Authentication URL http://saml10-12.caf.eauth.enspier.net/siteminderagent/redirectj

**Don't forget to set up a policy to protect this Authentication URL.

Name	User Class
all	all

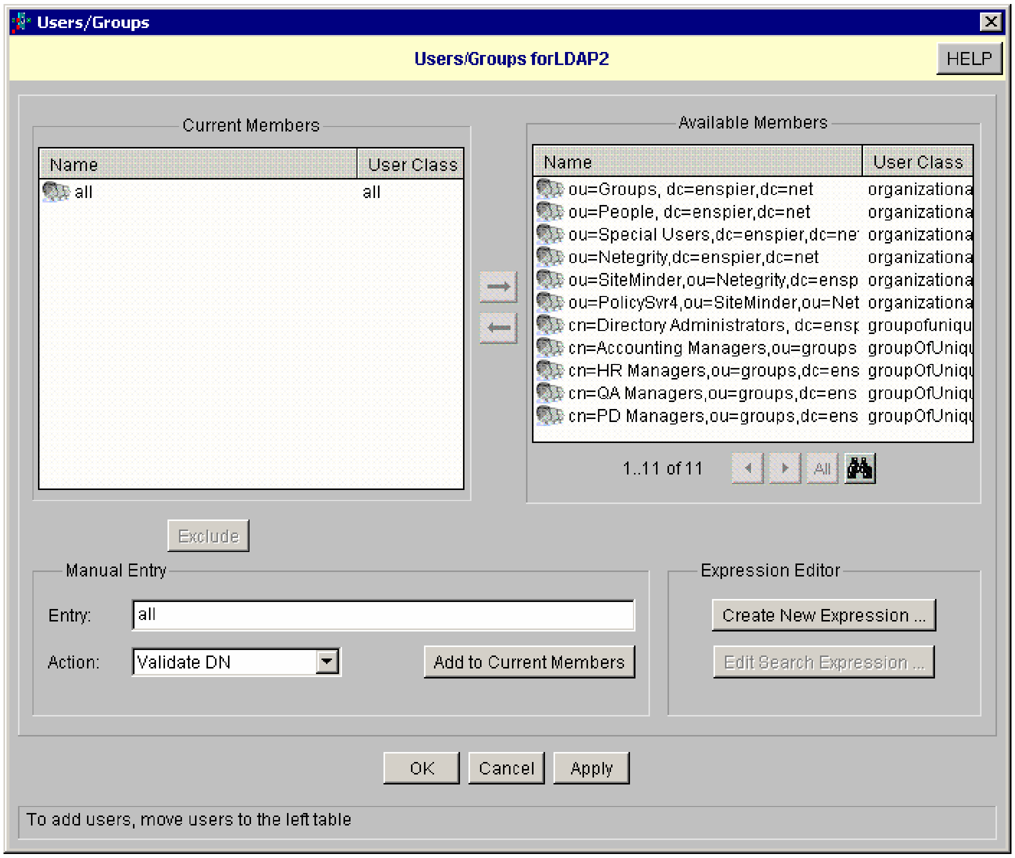
□ Allow Nested Groups

(LDAP2 is an Authentication and Authorization Directory)

Affiliate win1670.fedtraveler.com

Figure 20-13: Affiliate Properties – LDAP2

The Users/Groups screen will appear as shown in Figure 20-14. To add a single user, select the user from the **Available Members** column and click on the 🡐 button. You could also type **all** in the **Entry** field and click **Add to Current Members**. Next, select **Apply** and then **OK** when complete.



Users/Groups

Users/Groups forLDAP2

Current Members

Name	User Class
all	all

Available Members

Name	User Class
ou=Groups, dc=enspier,dc=net	organizationa
ou=People, dc=enspier,dc=net	organizationa
ou=Special Users,dc=enspier,dc=ne	organizationa
ou=Netegrity,dc=enspier,dc=net	organizationa
ou=SiteMinder,ou=Netegrity,dc=ensp	organizationa
ou=PolicySvr4,ou=SiteMinder,ou=Net	organizationa
cn=Directory Administrators, dc=ensp	groupofuniqu
cn=Accounting Managers,ou=groups	groupOfUniqu
cn=HR Managers,ou=groups,dc=ens	groupOfUniqu
cn=QA Managers,ou=groups,dc=ens	groupOfUniqu
cn=PD Managers,ou=groups,dc=ens	groupOfUniqu

1..11 of 11

Manual Entry

Entry: all

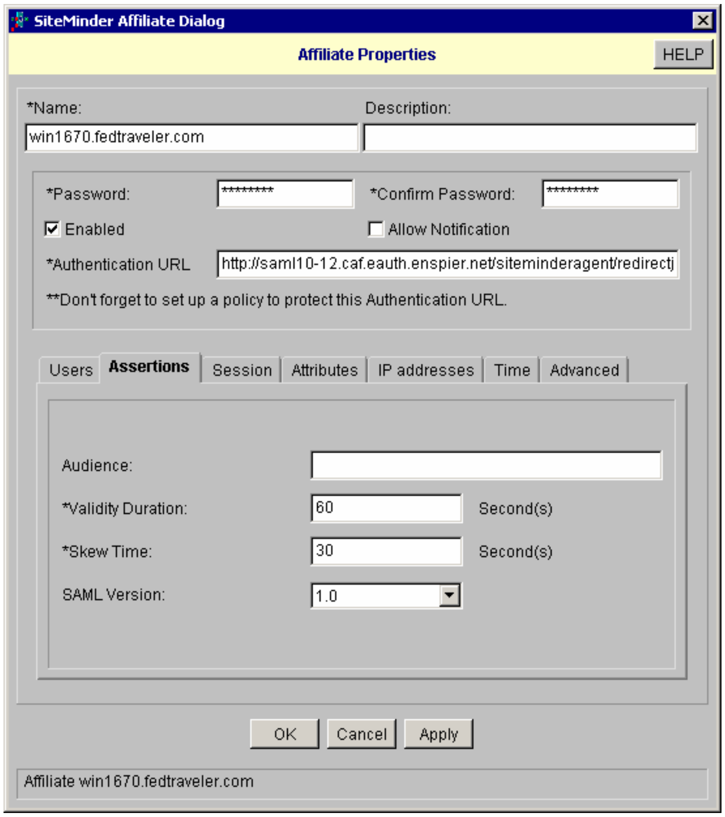
Action: Validate DN

Expression Editor

To add users, move users to the left table

Figure 20-14: Users/Groups

Next, verify that SAML 1.0 has been set. As demonstrated in Figure 20-15, click on the **Assertions** tab from the Affiliate Prosperities screen. The **SAML Version** pull down should be set to 1.0. Select **Apply** when complete.


SiteMinder Affiliate Dialog

Affiliate Properties

*Name: win1670.fedtraveler.com

Description:

*Password: ********

*Confirm Password: ********

☑ Enabled

□ Allow Notification

*Authentication URL: http://saml10-12.caf.eauth.enspier.net/siteminderagent/redirectj

**Don't forget to set up a policy to protect this Authentication URL.

Audience:

*Validity Duration: 60 Second(s)

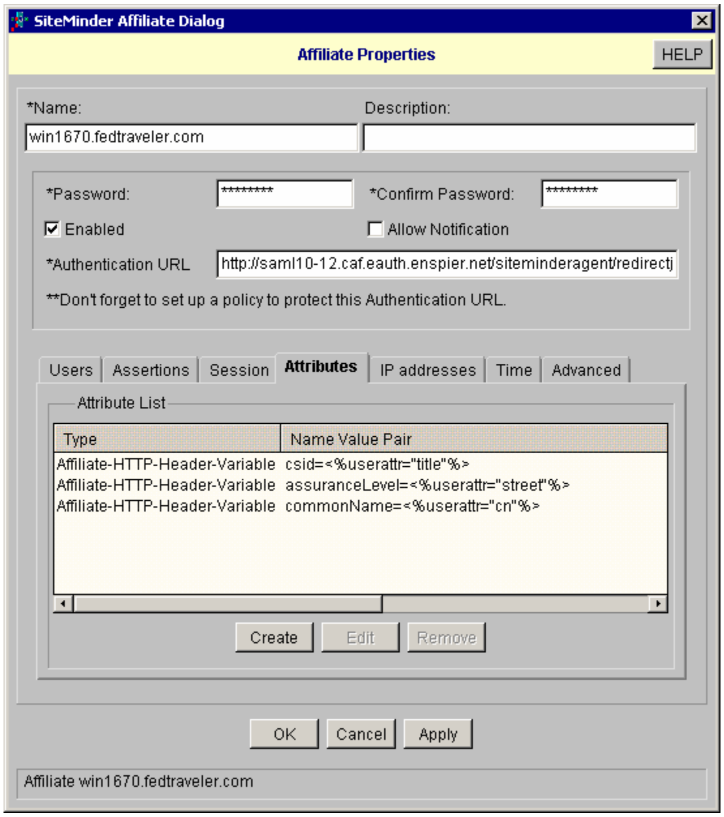
*Skew Time: 30 Second(s)

SAML Version: 1.0

Affiliate win1670.fedtraveler.com

Figure 20-15: Affiliate Properties - Assertions

Once you have verified SAML 1.0 has been set, click on the **Attributes** tab as demonstrated in Figure 20-16. The Attributes tab is where LDAP attributes are mapped to the SAML assertion attributes. Select the **Apply** button when complete.



*Name: win1670.fedtraveler.com

Description:

*Password: ********

*Confirm Password: ********

☑ Enabled

□ Allow Notification

*Authentication URL http://saml10-12.caf.eauth.enspier.net/siteminderagent/redirectj

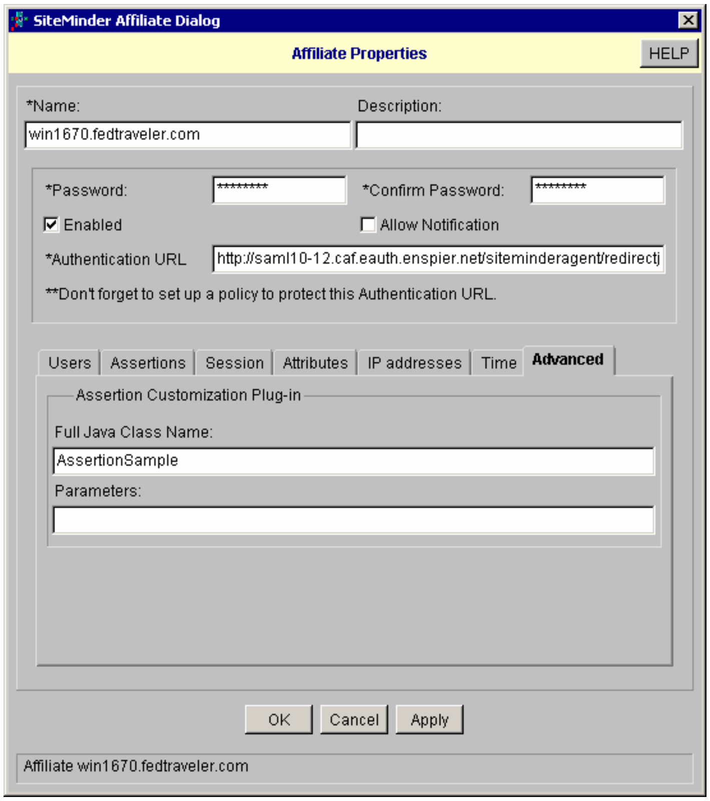
**Don't forget to set up a policy to protect this Authentication URL.

Type	Name Value Pair
Affiliate-HTTP-Header-Variable	csid=<%userattr="title"%>
Affiliate-HTTP-Header-Variable	assuranceLevel=<%userattr="street"%>
Affiliate-HTTP-Header-Variable	commonName=<%userattr="cn"%>

Affiliate win1670.fedtraveler.com

Figure 20-16: Affiliate Properties - Attributes

Next, click on the **Advanced** tab as demonstrated in Figure 20-17. **AssertionSample** provided in the Full Java Class Name field refers to the name of the plug-in developed to customize our SAML assertion. You may have a different plugin. Select **Apply** and then **OK** when complete.



*Name: win1670.fedtraveler.com

Description:

*Password: ********* *Confirm Password: *********

☑ Enabled □ Allow Notification

*Authentication URL http://saml10-12.caf.eauth.enspier.net/siteminderagent/redirectj

**Don't forget to set up a policy to protect this Authentication URL.

Assertion Customization Plug-in

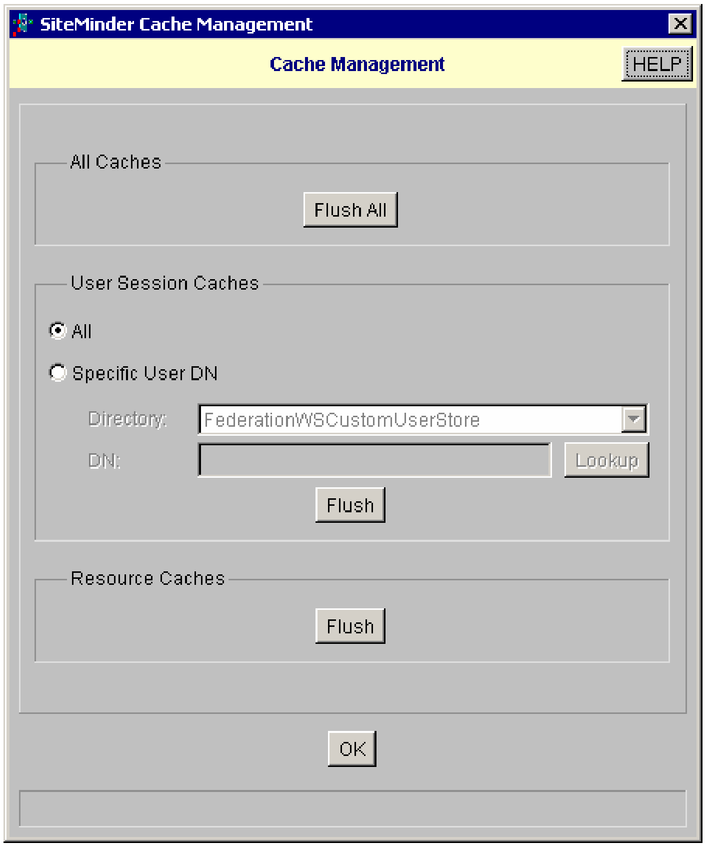
Full Java Class Name: AssertionSample

Parameters:

Affiliate win1670.fedtraveler.com

Figure 20-17: Affiliate Properties - Advanced

Next, from the SiteMinder 6.0 Administration screen, click on **Tools > Manage Cache**. The Cache Management screen will appear as shown in Figure 20-18. Click on the **Flush All** button and then select **OK**. This will complete the process of configuring an AA.

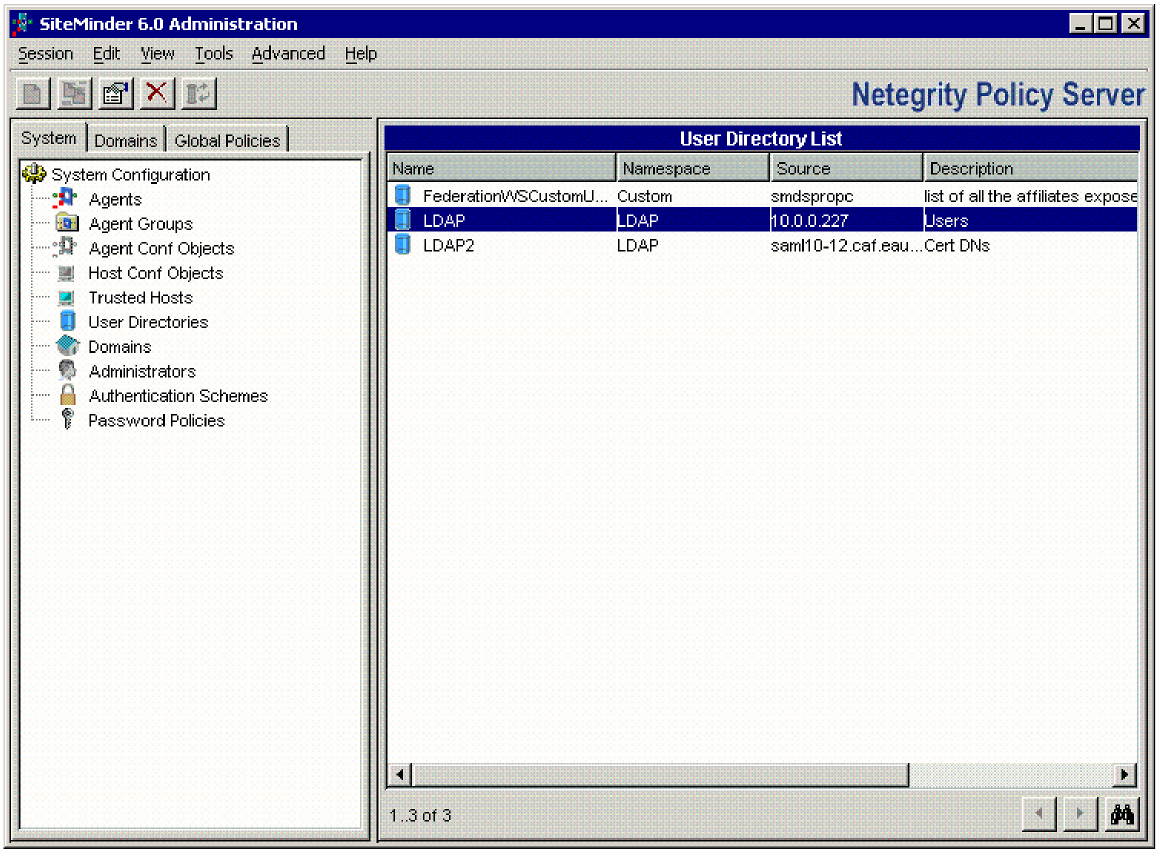


● All
○ Specific User DN
Directory: FederationWSCustomUserStore
DN:

Figure 20-18: Cache Management

2.3 Configure a Partner CS

Open Netegrity Policy Server 6.0 and login as described in Figure 20-1 and 20-2. Once the SiteMinder 6.0 Administration screen has opened, click on the **System** tab (left side of the screen) and then select **User Directories**. The User Directory List screen will appear as shown in Figure 20-19. To create a new Directory resource right click on **User Directories** and select **Create Directory**. Creating a directory maps the subject from the SAML assertion to the uid of the user in you backend LDAP data store.

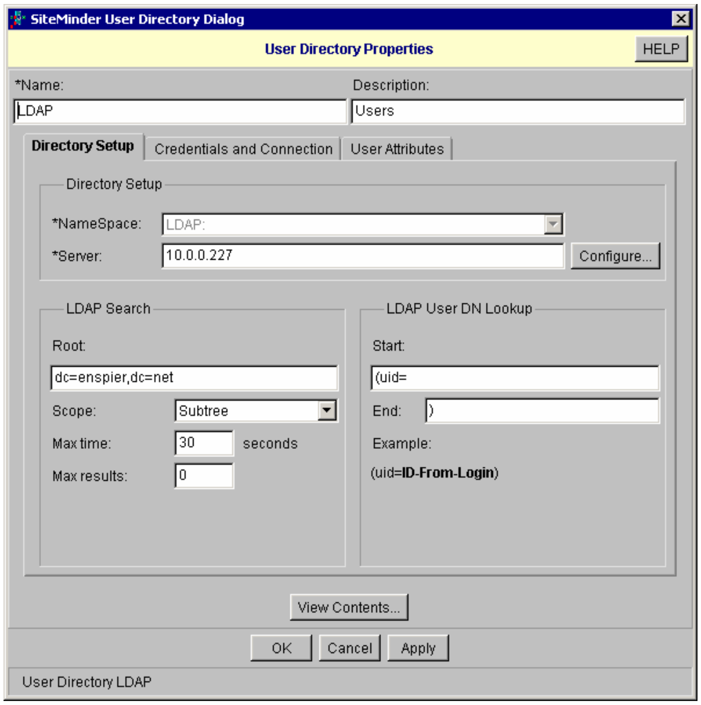


User Directory List

Name	Namespace	Source	Description
FederationWSCustomU...	Custom	smdspropc	list of all the affiliates expose
LDAP	LDAP	10.0.0.227	Users
LDAP2	LDAP	saml10-12.caf.eau...	Cert DNs

Figure 20-19: User Directory List

The User Directory Properties screen will appear as shown in Figure 20-20. Next, select the **Directory Setup** tab and provide all appropriate configuration information as demonstrated below.


SiteMinder User Directory Dialog
User Directory Properties
HELP
Directory Setup
Credentials and Connection
User Attributes
Configure...
View Contents...
OK
Cancel
Apply

*Name: LDAP

Description: Users

Directory Setup

*NameSpace: LDAP:

*Server: 10.0.0.227

LDAP Search

Root: dc=enspier,dc=net

Scope: Subtree

Max time: 30 seconds

Max results: 0

LDAP User DN Lookup

Start: (uid=

End:)

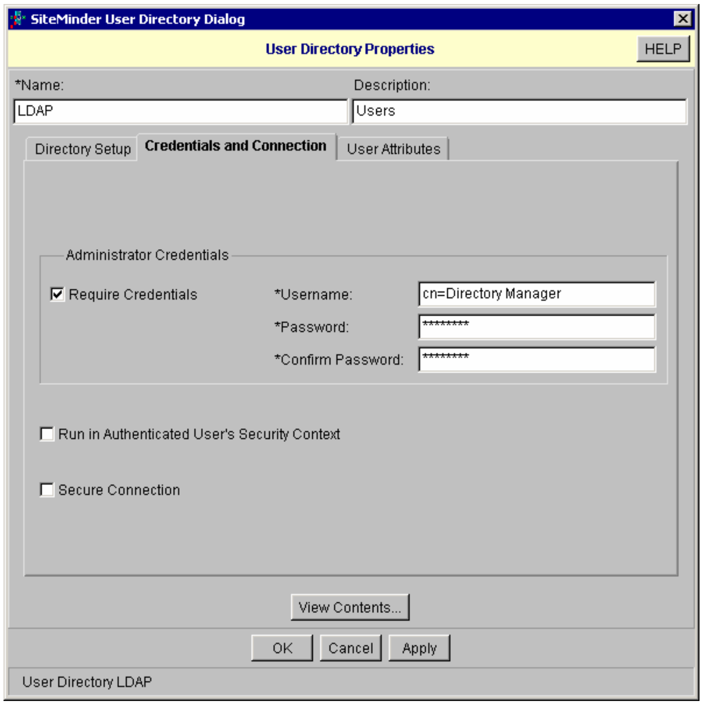
Example:

(uid=**ID-From-Login**)

User Directory LDAP

Figure 20-20: User Directory Properties

Next, click on the **Credentials and Connections** tab enter all appropriate configuration information as demonstrated in Figure 20-21. If desired, you can click **View Contents** to verify connection and that the policy server can connect to the LDAP server. The User Attributes tab contents are all defaults and no additional configuration information is needed. Select **Apply** and then **OK** when complete.



SiteMinder User Directory Dialog

User Directory Properties

*Name: LDAP

Description: Users

Administrator Credentials

☑ Require Credentials

*Username: cn=Directory Manager

*Password: ********

*Confirm Password: ********

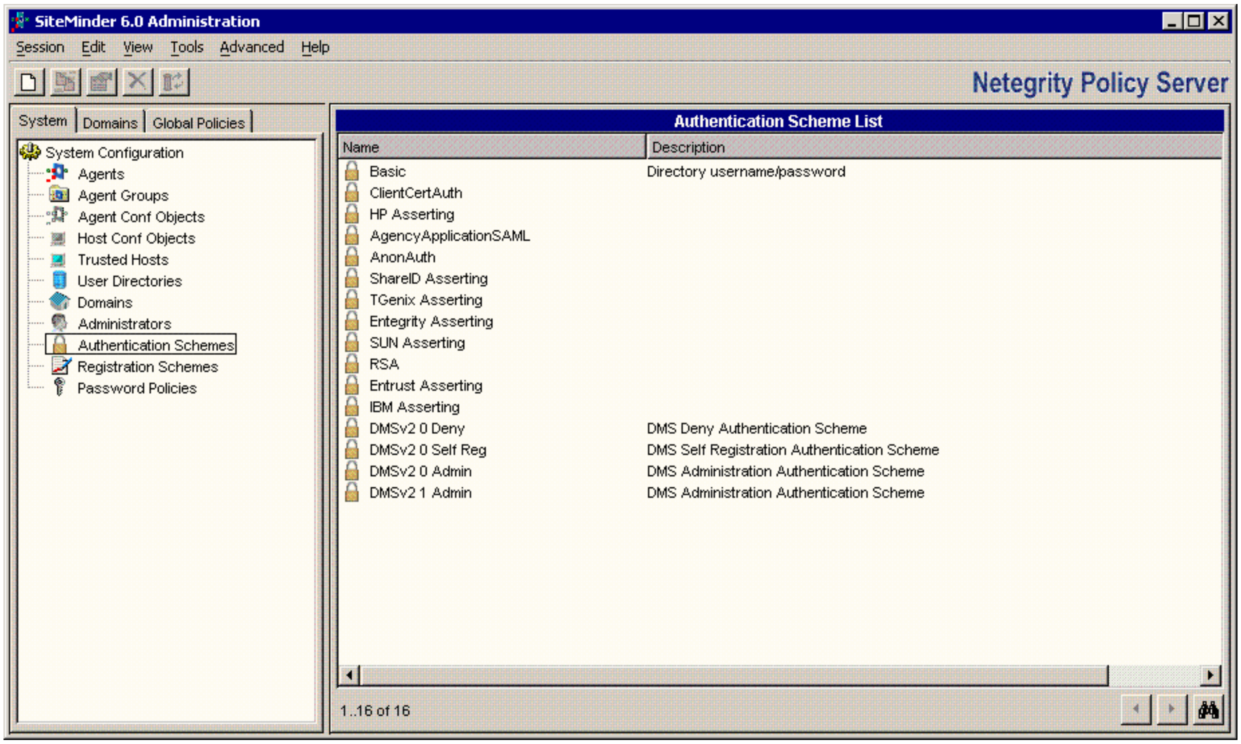
□ Run in Authenticated User's Security Context

□ Secure Connection

User Directory LDAP

Figure 20-21: User Directory Properties – Credentials and Connections

Next, from the SiteMinder 6.0 Administration screen, click on the **System** tab (left side of the screen) and then select **Authentication Schemes** as demonstrated in Figure 20-22.



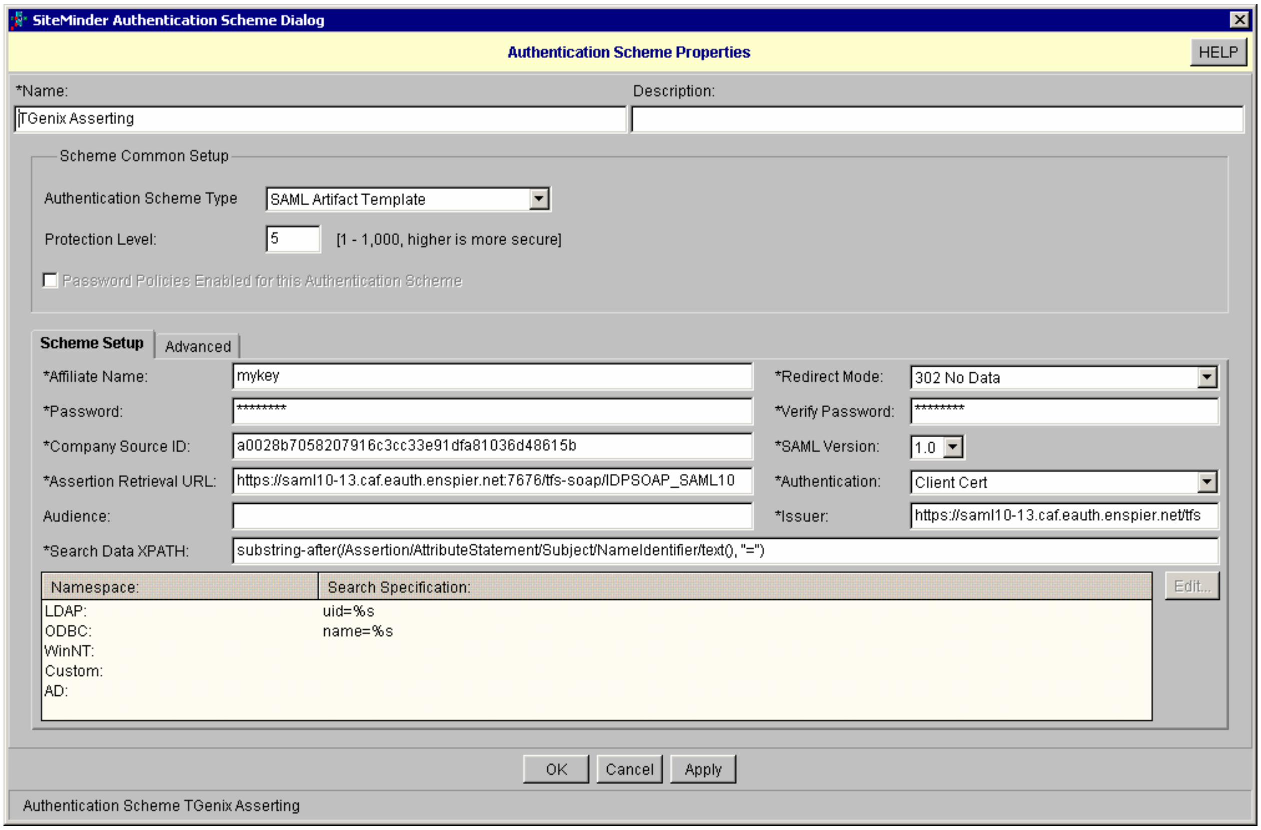
Authentication Scheme List

Name	Description
Basic	Directory username/password
ClientCertAuth	
HP Asserting	
AgencyApplicationSAML	
AnonAuth	
ShareID Asserting	
TGenix Asserting	
Entegrity Asserting	
SUN Asserting	
RSA	
Entrust Asserting	
IBM Asserting	
DMSv2 0 Deny	DMS Deny Authentication Scheme
DMSv2 0 Self Reg	DMS Self Registration Authentication Scheme
DMSv2 0 Admin	DMS Administration Authentication Scheme
DMSv2 1 Admin	DMS Administration Authentication Scheme

1..16 of 16

Figure 20-22: Authentication Schemes

Once you have selected Authentication Schemes, the Authentication Scheme Properties screen should appear as shown in Figure 20-23. Provide all appropriate configuration information as demonstrated below. The **Affiliate Name** and **Password** fields correspond to the alias and password of your server certificate in **<netegrity home>\webagent\affwebservices\AM.keystore**.


SiteMinder Authentication Scheme Dialog
Authentication Scheme Properties
HELP
Scheme Setup
Advanced
Edit...
OK
Cancel
Apply

*Name: TGenix Asserting

Description:

Scheme Common Setup

Authentication Scheme Type: SAML Artifact Template

Protection Level: 5 [1 - 1,000, higher is more secure]

□ Password Policies Enabled for this Authentication Scheme

*Affiliate Name: mykey

*Password: ********

*Company Source ID: a0028b7058207916c3cc33e91dfa81036d48615b

*Assertion Retrieval URL: https://saml10-13.caf.eauth.enspier.net:7676/tfs-soap/IDPSOAP_SAML10

Audience:

*Search Data XPATH: substring-after(/Assertion/AttributeStatement/Subject/NameIdentifier/text(), "=")

*Redirect Mode: 302 No Data

*Verify Password: ********

*SAML Version: 1.0

*Authentication: Client Cert

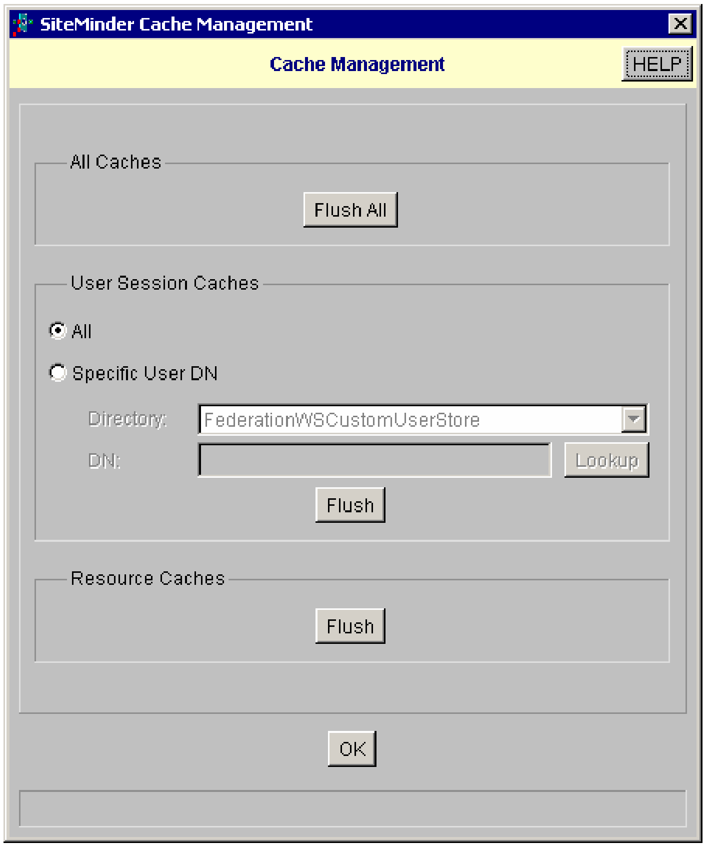
*Issuer: https://saml10-13.caf.eauth.enspier.net/tfs

Namespace:	Search Specification:
LDAP:	uid=%s
ODBC:	name=%s
WinNT:	
Custom:	
AD:	

Authentication Scheme TGenix Asserting

Figure 20-23: Authentication Scheme Properties

Next, from the SiteMinder Administration screen, click on **Tools** > **Manage Cache**. The Cache Management screen will appear as shown in Figure 20-24. Click on the **Flush All** button and then select **OK**. This will complete the process of configuring a CS.



● All

○ Specific User DN

Directory: FederationWSCustomUserStore

DN:

Figure 20-24: Cache Management